This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/60 — A1

(11) International Publication Number: WO 00/55777

(43) International Publication Date: 21 September 2000 (21.09.00)

(21) International Application Number: PCT/NO00/00092

(22) International Filing Date: 16 March 2000 (16.03.00)

(30) Priority Data:
1999 1278 16 March 1999 (16.03.99) NO

(71) Applicant *(for all designated States except US)*: JØLSTAD, Lars [NO/NO]; Kirsebærstien 15, N–1349 Rykkinn (NO).

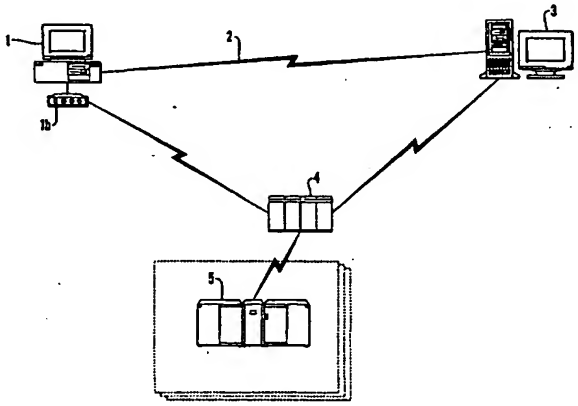
(71)(72) Applicant and Inventor: KRUGLENKO, Ilya [RU/ES]; Calle Calvario, 62, E–03580 Alvaz Del Pi, Alicante (ES).

(74) Agent: ONSAGERS AS; P.O. Box 265 Sentrum, N–0103 Oslo (NO).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND SYSTEM FOR SECURE ON–LINE SHOPPING



(57) Abstract

A method for performing secure on–line transactions in a system which at least includes one or more customer computers (1), one or more vendor computers (3), a payment system (4) with which the vendors are registered, and a payment authorization system (5), is described. The method includes such steps as transferring information regarding available products from a vendor computer (3) to a customer computer (1), and transferring order information to the vendor computer (3) either directly or by way of the payment center (4). Further the method includes sending payment information from the customer computer (1) to the payment center (4). Following an approval from the payment authorization system (5), the payment system (4) sends a voucher to the customer computer (1), and a delivery approval accompanied by relevant order information to the vendor computer (3). The vendor then delivers the ordered product, possibly in exchange for the voucher. After receiving a claim from the vendor that the delivery has been made, possibly including the voucher, the payment system (4) handles the debiting of the customer and the crediting of the vendor. Also described is a system for implementing the described method.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Method and system for secure on-line shopping

The present invention relates to a method and a system for secure on-line transactions. In particular, the invention relates to such transactions performed over a public communications network such as the Internet.

The phenomenal growth of the Internet has prompted more and more businesses to establish a presence on the Internet, primarily in the form of so called web pages. However, the expected growth of business actually conducted over the Internet has not shown a similar growth, and the main reason for this is that no satisfactory standard for payment of goods and services over the net has been established. Today the most convenient payment method is payment by credit card, but the transmission of card information over the Internet is insecure and is generally discouraged by card operators.

Other disadvantages with the use of credit cards over the Internet include the fact that the vendor or service provider with which a customer wants to do business must be registered with the card operator who has issued the customer's credit card in order to be able to accept it. Furthermore, even if the credit card information is transferred to the vendor without being compromised, the customer may not know if the vendor can be trusted not to use the credit card information unfairly, and whether the vendor stores the credit card information gathered from his customers in a secure manner. In many cases it may turn out to be easier to steal an entire database of credit card information through a break in into a vendor's system than to intercept individual card data transmitted over the Internet.

Alternatives to ordinary credit card payment include different forms of electronic cash and cryptographic systems that simply have turned out to be to complex to appeal to the general customer.

With the systems mentioned above, the disadvantage is usually with the customer. Compromised credit card information, dishonest vendors that charge but do not deliver and goods that are damaged in transit and delivered in a poor condition after payment has been made in full, leaves the customer in a situation where he or she will want to be reimbursed, something that can prove difficult. On the other hand, payment on delivery will often prove

dissatisfactory to the vendor who will suffer through late or no payment, or the refusal of the customer to accept the goods.

To complicate matters further, the customer and the vendor often resides in different countries. Any conflict relating to problems as the ones mentioned above will therefore be difficult and expensive to resolve, and due to different legislation in different countries, the parties may not be aware of what rights and duties they actually have.

The present invention relates to a payment system that provides customer as well as vendor with higher security without introducing unnecessary burdensome tasks for either. Through the steps of the method of the invention, a customer is able to pay for goods or services using his credit card with a greatly reduced risk of having his credit card information compromised. At the same time, the method provides the vendor with an opportunity to accept credit card payment without actually being registered with each and every operator of credit cards, debit cards, smart cards and the like. When in the following description reference is made to credit cards, it must be understood that this is intended to cover any kind of credit card, debit card, credit or debit account, smart card or the like.

The particular benefits of the present invention are achieved through the steps described in claim 1, respectively in claim 18. A system for implementing the method is described in claim 35. Additional steps and features are described in the dependent claims.

According to the invention, a customer has access to a computer network, such as the Internet, through his computer. Also connected to this computer network is a number of computers containing information regarding goods and/or services offered by any number of providers. E.g. this information can be available through so called web pages set up by the providers, hereinafter referred to as vendors, on computers that act as web servers. Currently the most common way of presenting such information is through hypertext markup language (html) files (often combined with the use of scripts (Perl/CGI) and Java applets), the hypertext transfer protocol (http) and TCP/IP (Transmission Control Protocol/Internet Protocol). Other ways of making the information available to customers is of course possible, through any number of data formats and communication protocols available. To one

skilled in the art it will be obvious that other ways of presenting and transferring the relevant information are possible.

When a customer retrieves information regarding the goods or services offered by a vendor from the computer network, this information will be presented to him on his computer. The customer then selects any product or service he wants to purchase, and information regarding this is sent from the customer's computer to the vendor's computer along with any information necessary for shipment, such as the customer's name and address and/or shipment address. This information can be provided by the customer at the time, or it can be stored in his computer ahead of time, always ready to be added to any transmission of ordering information. If the customer is already registered with the vendor, the customer's name and address may already be stored in the vendor's computer, and the customer information transmitted will in this case only include a reference to this information. This may be implemented through a so called cookie stored on the user's computer.

When the vendor receives the ordering information, information required for the processing of the payment is sent back to the customer. This information may include the total amount the customer is supposed to pay, a reference identifying the filed order, a reference identifying the vendor and any other relevant information, such as specification of goods ordered etc. The vendor does not have to be registered with any credit card company, but he must have an account with a payment system that consists of one or more payment centers. The vendor identification identifies the vendor uniquely to this payment system.

At this point, the customer terminates the connection to the vendor. If the customer is connected to the computer network by a modem, the modem simply hangs up. The customer then enters the necessary payment information, which can for example include credit card number, expiration date, or, if this information is pre-stored on his computer on a preferably encrypted file, he simply confirms his intention to pay for the goods or services he has just ordered. A connection is then established between the customer's computer and a computer at a designated payment center which constitutes or is part of the above mentioned payment system. This connection is not established over the public computer network used for communication between the customer and the vendor, but through a

relatively secure data channel. for example the customer's modem dials up a direct connection to the payment center using the public telephone network. and preferably encrypted. Alternatively the information is sent over a public computer network. but strongly encrypted. and possibly in the form of an e-mail message. The ordering information along with the credit card information is now transferred to the payment center. This information may then include vendor identification. order identification. total amount. customer name. address and credit card information and the customer's e-mail address. and constitutes a payment approval request.

After receiving and. if necessary. decrypting this request. the payment center directly or through the payment system of which it is part. requests payment authorization from the credit card operator indicated by the customer's credit card information. or from some authorization authority approved by the credit card operator. This authorization authority will hereinafter be referred to as the payment authorization system. and this may include a credit card operator. a debit card operator or anyone else with whom the customer has set up some kind of an account. as well as any authority authorized one or more such entities. The payment system is able to choose the relevant authority out of any number of such authorities based on customer information such as for example credit card information. The request is preferably transmitted over a secure connection. such as a dedicated line.

If the payment system does not receive the requested authorization. the transaction is canceled. Information regarding this could be transmitted to the customer and/or the vendor. or the payment system may simply neglect to respond and the ongoing transaction may be canceled at the customer and vendor locations after a set time limit. Anyone with ordinary skill will realize that there are a number of ways to cancel the ongoing transaction. and that choosing one over another is simply a matter of implementation.

If on the other hand the payment center does receive the requested authorization. the following actions are performed by the payment system. First a unique voucher is generated by the payment system. based on the relevant transaction data. This voucher is transferred to the customer over the relatively secure line between the customer and his local payment center. This connection is then terminated.

The payment system then transmits a shipment approval to the vendor. It is important that the vendor is able to verify that the shipment approval actually originated with the payment system, so the shipment approval will preferably be signed digitally. This can be done in a number of ways, e.g. through use of a public key/private key system, through some mutually trusted verification agency or in any other manner of digital signature known in the art. Since the information transmitted from the payment system to the vendor does not contain confidential information, the connection can be made through a public network such as the Internet. If necessary, the payment system then terminates the connection with the vendor and waits for funds to be transferred from the credit card operator.

Following this, the vendor delivers the purchased goods or services in exchange for the voucher. If the goods or services purchased are deliverable over the Internet, such as software or information, the exchange can be implemented automatically. If this is not possible, the customer will hand over the voucher upon delivery of the goods or services. The vendor will of course not have precise knowledge of the voucher in advance. He will however preferably be able to verify that the voucher is indeed issued as part of the relevant transaction. This can be done by including the transaction identification in the voucher, since this will not be known to any third party trying to obtain the goods or services by presenting a false voucher. It is also possible for the payment system to transfer some information relating to the voucher along with the shipment approval, such as the checksum of the voucher number or some other means of verifying that the voucher is a voucher actually relating to the relevant transaction.

After the vendor transfers the voucher to the payment system, the amount authorized by the credit card company will be transferred to the vendor, possibly less a commission kept by the payment system and any possible fees or royalties to third parties as the result of any licenses or copyrights relating to the product.

In an alternative embodiment, the ordering information is not sent from the customer computer to the vendor computer directly, but to the payment system along with the payment information. The payment system then forwards this order information to the vendor along with the delivery approval upon receipt of the requested payment authorization. the delivery is

then made by the vendor solely based on information received form the payment system.

The invention will now be described in further detail by way of examples and with reference to the enclosed drawings.

Fig. 1 shows a possible configuration of an on-line shopping system using the method according to the present invention.

Fig. 2 shows an alternative configuration of an on-line shopping system where the payment system consists of several local payment centers.

Fig. 3 shows a flowchart of the method according to the present invention.

Fig. 4 shows a flowchart of an alternative method according to the present invention.

Referring now to Fig. 1, a system for on-line shopping is shown. The system includes a customer's computer 1 connected to a public network 2 such as the Internet. Also connected to this network is a number of vendors' computers 3. Only one such computer is shown. These computers contain information presenting goods and/or services available from the vendors, e.g. in the form of web pages. Based on the information available to him in this way, a customer can file an order with the vendor by transmitting this order to the vendor's computer system. This may not necessarily be the same computer used to present the product information: it may also be a different computer set up to handle orders. Included in the on-line shopping system is also a payment system 4. This system is set up to handle payment, and all vendors must be registered with this payment system. A vendor registered with the payment system will receive a unique vendor ID. The system may be a centralized system run by only one operator, or it may be a network of payment centers run by several operators. Of course it may also be run by one operator, but consist of several distributed local payment centers. In the following description, payment system will be used to refer to the whole payment system whether this is distributed or centralized, and payment center will be used to refer to the local payment center where vendor's are registered and to which customers connect, whether such a center constitutes the whole of the payment system or only a part of it.

The payment system 4 is able to communicate with one or more payment authorization systems 5. The dotted lines surrounding the payment authorization system 5 shown in Fig. 1 indicates that there may be only one such authorization center, or there may be several, e.g. one for each credit card the payment system is able to accept.

The communication channel between the customer computer 1 and the payment system 4 is preferably a relatively secure line, such as a dial up connection using the customers modem 1b. The communication channel between the payment system 4 and the payment authorization center is preferably a secure channel such as a dedicated line. The communication channel between the payment system 4 and the vendor computer 3, however, need normally not be a secure line, and can be a public network such as the Internet.

Reference is now made to Fig. 2, where a possible alternative configuration of an on-line shopping system is shown. Reference numbers identical to those found in Fig. 1 refer to the same or similar parts of the system. In this configuration, the payment system 4 consists of several local payment centers 11, 12 as well as a database 13 and a computer network 14 connecting these. In this case, when a customer connects to the payment system 4, he connects to his local payment center 11. In this way he will only have to dial a local number if the connection to the payment system 4 is a dial up connection. A vendor wishing to register with the payment system 4, registers with his local payment center 12, and receives a vendor ID that identifies him uniquely to the payment system 4. It is of course possible for all the local payment centers 11, 12 to distribute all the vendor IDs they have allocated to all the other payment centers 11, 12, so that all local payment centers at all times have a complete list of all registered vendors. However, it is also possible to store this information in one or more databases 13 accessible by the payment centers 11, 12. In this case, the database may contain all vendor IDs or only a table relating a given vendor ID to the right payment center. Information from the payment system 4 to a given vendor will then be sent to the vendor's payment center to be distributed.

The network 14 connecting the local payment centers 11, 12 and database(s) 13 that constitutes the payment system 4, will normally not need to be a secure network, since all confidential information is transmitted between the

customer computer 1 and the local payment center 11 and between the local payment center 11 and the payment authorization system 5. It is however possible to modify the payment system by distributing tasks in a different manner, and the need for secure communication may then arise within the payment system. It is for instance possible to let the local payment center connect to the payment authorization center through other computers in the payment system.

Referring now to Fig. 3, the method according to the present invention will be described in detail.

A potential customer is connected to a public computer network 2 such as the Internet, through his computer 1. In a first step 101, the customer retrieves information that is available on the network from a vendor computer 3. As already mentioned, this information may be presented in the form of HTML documents, or in any other convenient format, and transferred over the computer network by way of any well known protocol, such as TCP/IP.

In a next step 102, the customer selects any goods and/or services he might be interested in, and transfers order information to the vendor. Again there are several options for transferring this information. If the customer is already registered with the vendor, he may be identified to the vendor e.g. by so called cookies already stored on his computer and the customer may simply click on the items he wants to purchase. Other options include for example filling in an order form with necessary order data such as customer name, address and delivery address, and pressing a send button. The information may be transferred by way of the http protocol, or by any other suitable protocol.

When in a following step 103 the vendor computer 3 receives the order information from the customer computer 1, an order ID is generated and transferred to the customer computer 1 along with a vendor ID, a total amount and any other relevant information.

When the customer has received this information, he may disconnect from the public computer network 2 that interconnects his computer 1 and the vendor computer 3. This may be done automatically by software running on his computer 1. When the customer is ready to pay, he will be presented with a dialog box where he is requested to fill in personal information such as

name. address and credit card information (referred to collectively as customer ID in Fig. 3). Some of this information may already be present in the information transmitted from the vendor computer to the customer computer, and in that case the customer will only have to supply the information not already available in this way. At the very least this will include his credit card information. This payment information may already be stored on the customer computer in a preferably encrypted file. In that case all the customer has to do is to confirm his intention to pay. Alternatively the customer may be registered with the payment system 4 or a payment authorization system 5 with a debit account. a credit account or something similar. but for convenience it will be assumed in the following description that he is paying with a credit card. Actually any combination of information being entered by the customer. information being extracted from the information received from the vendor computer 3. information being pre stored on the customer computer 1 and information being pre stored in the payment system 4 or payment authorization system 5 is possible. The main thing is to make sure that the credit card information is not made available to the vendor and that the order information from the vendor is accurate when processed by the payment system.

The payment information entered by the customer. along with the vendor ID, the order ID and the total amount. is then transferred 104 to the payment system 4. preferably in encrypted form.

Upon receiving this information. the payment system 4 requests authorization from the payment authorization system 5 by transferring 105 credit card information and total amount to the payment authorization system 5. The payment authorization system 5 may be one out of many, depending on what system has authority to authorize payment on the credit card specified by the customer.

In a next step 106. the payment system will either receive the requested authorization. or authorization is denied. If authorization is denied, the transaction is terminated 107. This may be communicated to the user and possibly also the vendor. or the transaction may simply be terminated in the different computers if the transaction does not proceed within a given time.

If the transaction is authorized by the payment authorization system 5, the payment system in a next step 108 generates a voucher and transfers this to the customer computer. The connection between the payment system and the customer computer may then be terminated. The payment system also generates a delivery approval and transfers this to the vendor. If the payment system is distributed, the payment center 11 that is handling the transaction may have to look up the address of the vendor in a database 13. This address may include a network address for the vendor computer, an actual mail address, an e-mail address, a telefax number or any other vendor address to which the payment system 4 is able to send a message. Based on the vendor ID the payment center 11 may be able to retrieve this address directly, or the vendor ID will only refer to the address of another payment center 12. If the latter is the case, the payment center 11 handling the transaction will transfer the delivery approval to the payment center 12 referred to by the vendor ID, and this payment center 12 will forward the delivery approval to the vendor 3. The delivery approval does not contain confidential information, and may therefore be transferred over a public network such as the Internet. However, it is important that the vendor is able to verify that the delivery approval was sent by the payment system 4 and not by any dishonest customer other unauthorized source. The delivery approval is therefore preferably signed by a digital signature. Such a signature can be generated in a number of well known ways, e.g. by way of a public key/private key encryption algorithm.

In the following step 109, the vendor delivers goods and/or services to the customer, preferably in exchange for the voucher. If the goods and/or services constitutes information, software or something else that may be transferred over a computer network, this exchange may be done automatically. If not, the goods or services may be exchanged for the voucher manually. In some implementations of the invention it may however be necessary to forego the exchange and simply deliver the goods and/or services simply based on the delivery information and the delivery approval. This might for instance be the case when the delivery address is not the same as the address of the customer.

After receiving the voucher, the vendor transfers 110 this to the payment system. When the payment system 4 receives the voucher, the funds will be transferred to the vendor, and the transaction is completed. If the vendor has not received the voucher, he will simply make a claim that the delivery has

been made. In this case the payment center will credit the vendor for example after a given period of time unless the customer does not make a counterclaim stating that the ordered goods and/or services has not been delivered.

Figure 4 shows a flowchart that represents an alternative to the embodiment as described with reference to Fig. 3. According to this embodiment, the customer receives information from the vendor regarding available goods and/or services as well as prices in a first step 201. This information includes vendor information such as a vendor ID. Based on this information the customer selects 202 goods and/or services he wants to purchase.

When the customer is ready to order, he provides the necessary customer information as mentioned above, and this information along with the ordering information is transferred 203 to the payment system. In this case the ordering information regarding the ordered product is not filed directly with the vendor, but with the payment system.

In a next step 204 the payment system requests payment authorization in the same manner as described above. If the payment system receives positive payment authorization information in step 205, a voucher is generated 207 and transferred to the customer computer as described above. Likewise a delivery approval is generated and transferred to the vendor computer, along with the ordering information, such as delivery address and information identifying the ordered goods and/or services.

After the vendor receives the order information and the delivery approval, the rest of the process proceeds as described above. The vendor delivers 208 the ordered goods and/or services, preferably in exchange for the voucher. After having made the delivery, the vendor transfers 209 a claim, preferably, including the voucher, to the payment center. The payment system then credits 210 the vendor, possibly after a certain period that gives the customer a chance to claim that the goods and/or services have not been delivered.

This particular embodiment is particularly convenient when the vendor is selling products that are deliverable over a public computer network such as the Internet. The customer may then download such a product in a trial version, possibly as part of retrieving information from the vendor in step 201, or in advance of the whole process described. This trial version.

preferably along with the vendor information and price information, may be downloaded from any location, not necessarily from a computer operated by the vendor. (For the purposes of this description, such a computer will still be referred to as a vendor computer simply because it contains information from the vendor.) Such a product may include computer software, music, data, multimedia presentations etc. The goods actually purchased through the method according to the present invention, and delivered from the vendor after receipt of a delivery approval from the payment system, may then be a key that unlocks the trial version after the expiry of the trial period and converts it to a regular version of the product. It should be pointed out that this scheme may be used also regarding trial versions that are distributed by other means, such as on CD ROM or diskettes. And of course the second embodiment may also be used for any other goods or services as an alternative to the first embodiment.

It is important to note some of the security features as well as the flexibility provided by the method according to the present invention. Vendors that wish to offer their products over a computer network such as the Internet only have to set up an account with the payment system, without any approval from credit card companies. The payment system, however, will be registered with credit card companies, and the credit card companies makes the payments to the operator or one of the operators of the payment system. In this way, any company, small or large, or even a private individual, that wishes to sell almost anything over the Internet, may do so fairly simply. Furthermore, since funds are transferred from the credit card company to the payment system, the customer may not withhold payment by not handing over the voucher after receiving the ordered goods and/or services. The payment will be held by the payment system until the voucher is received from the vendor. If the vendor does not receive the voucher in exchange for delivered goods, he may make a claim to the payment system, which may then hold the money until any conflict between customer and vendor has been resolved, or the payment system may release the payment to the vendor if the customer does not respond within a given time after having been notified that the vendor demands payment without being able to present the voucher.

On the other hand, if the customer never receives the ordered goods and/or services, he may make such a claim to the payment system which will then

return the funds to the customer, unless the payment system receives the voucher or a claim that delivery has been made from the vendor within a given time. In case of a conflict, the payment system may withhold the funds until the conflict has been resolved.

In order for the vendor to make sure that the voucher he is given in exchange for the goods or services is genuine, the voucher should identify the order ID, since this will not be known to any impostor trying to obtain the goods or services in the name of the actual customer. Additional security can be provided by including with the approval information transferred from the payment system to the vendor, information that allows for the authentication of the voucher. This may be in the form of a part of the voucher that may not be generated by an impostor, by a checksum that is generated from the voucher, or by a key that may be used to decrypt information hidden in the voucher.

To prevent the customer from changing the amount before transferring the payment information to the payment system, the order information transferred from the vendor computer to the customer computer and forwarded to the payment system by the customer may be tamper proof such that any modification to this information will be detected by the payment system. Alternatively, the delivery approval information transferred from the payment system to the vendor may include information on paid amount so that the vendor is able to confirm that the funds held by the payment system corresponds with the total amount for the given order. Any combination of such security functions may also be implemented, so that any transaction containing inaccurate information may be terminated as soon as possible.

Several modifications to the method as described above may be made within the scope of the present invention. For instance, any number of communication protocols may be used for transferring information between the different computers and systems that perform the method. Further, what above is described as being one computer, for instance the vendor computer, may in fact be several computers that are interconnected by some well known means and that perform different steps of the method. It should also be noted that the payment authorization system and the payment system may be operated by the same organization or legal entity, and may even be running on the same system or the same computer. If encryption and/or digital

signatures are used, any of the well known algorithms or methods known in the art may be employed as well as future improvements and modifications to such algorithms and methods.

Another possible modification that lies within the scope of the invention is to include certain contract information along with the order information transmitted from the vendor computer to the customer computer and forwarded to the payment system. This contract information may specify how a certain amount of the payment should not be credited the vendor, but some third party that collects royalty or some other fee from sales of a given product. In this case the third party, e.g. a publishing company, an artist, an inventor or anyone else who owns rights related to the product delivered by the vendor, will not be dependent on the honesty of the vendor, since all sales will involve the payment center. Further, the individual or organization claiming the fee will be able to check that the vendor actually sends the correct contract information as part of the order information simply by placing an order and checking the order information received from the vendor.

Regarding the actual transfer of funds to the vendor, this is mainly a matter of how the parties operating the method according to the present invention agree to operate. Funds may be transferred immediately upon receipt of the voucher, or a certain period of time after a claim has been made by the vendor and no counter claim has been made by the customer. It is also possible to wait until funds have actually been transferred from the credit card company to the payment system. A number of modifications to this scheme is possible and will be realized by anyone with the relevant skills for implementing the method according to the invention.

CLAIMS

1. Method for performing on-line transactions in a system which at least includes one or more customer computers, one or more vendor computers, a payment system with which the vendors are registered, and a payment authorization system, the method comprising the steps of

transferring information regarding available goods and/or services from a vendor computer to a customer computer over a first communication channel,

transferring information regarding goods and/or services to be ordered as well as customer information and delivery information necessary for the delivery of the goods and/or services, from said customer computer to said vendor computer over said first communication channel,

transferring information regarding payment of the ordered goods and/or services, including information identifying the particular order and the particular vendor, from said vendor computer to said customer computer over said first communication channel,

transferring information regarding payment settlement including customer identification, vendor identification and order identification as well as amount to be paid, from said customer computer to a payment system over a second communication channel,

transferring a request for a payment authorization including amount to be paid and customer identification, from said payment system to a payment authorization system over a third communication channel,

terminating the transaction if no such authorization is received from the payment authorization system, or after receiving such authorization, generating information representing a voucher that indicates that the customer has provided payment for the transaction identified by said order identification, and transferring this information from the payment system to the customer computer over said second computer channel, generating information approving delivery of the ordered goods and/or services and transferring this information from the payment system to said vendor computer over a fourth communication channel, and debiting the customer for said amount to be paid;

delivering the ordered goods and/or services from the vendor in accordance with the delivery information,

transferring a claim that the goods and/or services have been delivered, from the vendor to the payment system, and

crediting the vendor after receipt of said claim by the payment system.

2. Method according to claim 1, wherein

said first communication channel is a public computer network such as the Internet.

3. Method according to claim 1, wherein

said second communication channel is a relatively secure channel such as a dial up connection over the public telephone network.

4. Method according to claim 1, wherein

said second communication channel is a public computer network such as the Internet.

5. Method according to claim 1, wherein

said third communication channel is a secure channel such as a dedicated line.

6. Method according to claim 1, wherein

said fourth communication channel is a public computer network such as the Internet.

7. Method according to claim 1, wherein

the customer information transferred from the customer computer to the payment system includes credit card information or similar information identifying a customer debit account or a customer credit account.

8. Method according to claim 1, wherein

the information transferred from the customer computer to the payment system is encrypted.

9. Method according to claim 1, wherein

the payment system is constituted by one payment center, with which all vendors must be registered.

10. Method according to claim 1, wherein

the payment system consists of several payment centers that are geographically widespread but interconnected so that vendors need only be

registered with a local payment center, the information regarding any vendor being available to other payment centers through said interconnection.

11. Method according to claim 1, wherein
the information representing the voucher includes information uniquely identifying the ongoing transaction.

12. Method according to claim 1, wherein
the delivery of the goods and/or services from the vendor is done in exchange for the voucher.

13. Method according to claim 12, wherein
the claim that the goods and/or services have been delivered, includes the voucher received in exchange for the goods and/or services.

14. Method according to claim 12, wherein
the step of generating information approving delivery of the ordered goods and/or services includes a step of generating information that can be used to verify the authenticity of the information representing the voucher, such as a checksum, a part of the voucher information, or a key for decrypting information hidden in the voucher.

15. Method according to claim 1, wherein
the step of generating information approving delivery of the ordered goods and/or services includes a step of generating a digital signature that enables the vendor to confirm that the approval originated with the payment system.

16. Method according to claim 1, wherein
the information regarding payment of the ordered goods and/or services transferred from said vendor computer to said customer computer, further includes information regarding a contract between the vendor and a third party, said contract information being forwarded from the customer computer to the payment system along with the payment settlement information, and
the step of crediting the vendor includes a step of crediting said third party based on said contract information.

17. Method for performing on-line transactions in a system which at least includes one or more customer computers, one or more vendor computers, a

payment system with which the vendors are registered, and a payment authorization system, the method comprising the steps of

transferring information regarding available goods and/or services as well as information identifying the particular vendor of any such goods and/or services from a vendor computer to a customer computer over a first communication channel,

transferring information regarding goods and/or services to be ordered including vendor information and amount to be paid, as well as customer information and delivery information necessary for the delivery of the goods and/or services including customer identification, from said customer computer to a payment system over a second communication channel,

transferring a request for a payment authorization including amount to be paid and customer identification, from said payment system to a payment authorization system over a third communication channel,

terminating the transaction if no such authorization is received from the payment authorization system, or after receiving such authorization, generating information representing a voucher that indicates that the customer has provided payment for the transaction identified by said order identification, and transferring this information from the payment system to the customer computer over said second computer channel, generating information approving delivery of the ordered goods and/or services and transferring this information along with information regarding goods and/or services ordered and customer information and delivery information necessary for the delivery of the ordered goods and/or services from the payment system to said vendor computer over a fourth communication channel, and debiting the customer for said amount to be paid,

delivering the ordered goods and/or services from the vendor in accordance with the delivery information,

transferring a claim that the goods and/or services have been delivered, from the vendor to the payment system, and

crediting the vendor after receipt of said claim by the payment system.

18. Method according to claim 17, wherein

the goods and/or services to be purchased is a key that will unlock a trial version of another product after the trial period for said other product has expired.

19. Method according to claim 17, wherein
said first communication channel is a public computer network such as the Internet.

20. Method according to claim 17, wherein
said second communication channel is a relatively secure channel such as a dial up connection over the public telephone network.

21. Method according to claim 17, wherein
said second communication channel is a public computer network such as the Internet.

22. Method according to claim 17, wherein
said third communication channel is a secure channel such as a dedicated line.

23. Method according to claim 17, wherein
said fourth communication channel is a public computer network such as the Internet.

24. Method according to claim 17, wherein
the customer information transferred from the customer computer to the payment system includes credit card information or similar information identifying a customer debit account or a customer credit account.

25. Method according to claim 17, wherein
the information transferred from the customer computer to the payment system is encrypted.

26. Method according to claim 17, wherein
the payment system is constituted by one payment center, with which all vendors must be registered.

27. Method according to claim 17, wherein
the payment system consists of several payment centers that are geographically widespread but interconnected so that vendors need only be registered with a local payment center, the information regarding any vendor being available to other payment centers through said interconnection.

28. Method according to claim 17, wherein

the information representing the voucher includes information uniquely identifying the ongoing transaction.

29. Method according to claim 17, wherein

the delivery of the goods and/or services from the vendor is done in exchange for the voucher.

30. Method according to claim 29, wherein

the claim that the goods and/or services have been delivered, includes the voucher received in exchange for the goods and/or services.

31. Method according to claim 29, wherein

the step of generating information approving delivery of the ordered goods and/or services includes a step of generating information that can be used to verify the authenticity of the information representing the voucher, such as a checksum, a part of the voucher information, or a key for decrypting information hidden in the voucher.

32. Method according to claim 17, wherein

the step of generating information approving delivery of the ordered goods and/or services includes a step of generating a digital signature that enables the vendor to confirm that the approval originated with the payment system.

33. Method according to claim 17, wherein

the information regarding available goods and/or services transferred from said vendor computer to said customer computer further includes information regarding a contract between the vendor and a third party, said contract information being forwarded from the customer computer to the payment system along with the ordering information, and

the step of crediting the vendor includes a step of crediting said third party based on said contract information.

34. System for performing secure on-line transactions, comprising

one or more vendor computers connected to a public computer network and including means for storing information regarding goods and/or services offered by a vendor, means for upon request sending said information over said public computer network, means for receiving orders for goods and/or

services, means for receiving information representing a delivery approval relating to a given order, and means for sending a claim that the delivery of the ordered goods and/or services has been made,

one or more customer computers connected to a public computer network and including means for retrieving information regarding goods and/or services from said public computer network, means for sending information regarding an order for goods and/or services, and means for sending payment information including customer information, vendor information, order information and total amount,

a payment system including means for receiving said payment information, means for identifying a vendor address directly or indirectly based on the vendor information, means for requesting payment authorization information based on said customer information and said total amount, means for, upon receipt of positive payment authorization information, generating a voucher relating to said order information and transferring this voucher to the customer computer and generating delivery approval information and sending this to the vendor address identified by the vendor information, or terminating the transaction upon receipt of negative payment authorization, and means for receiving a claim that the delivery of the ordered goods and/or services has been made, and

a payment authorization system including means for receiving payment authorization requests including customer information and a total amount to be paid, means for generating payment authorization information based on said customer information and said total amount, and means for sending said payment authorization information.

35. System according to claim 34, wherein

said vendor computer further includes means for generating order information including said vendor information and a total amount, and said customer computer further includes means for receiving said order information from the vendor computer.

36. System according to claim 34, wherein

said payment system further includes means for receiving order information from said customer computer and means for forwarding this order information to the vendor computer along with said delivery approval information upon receipt of positive payment authorization.

37. System according to claim 34, wherein
said payment system is connected to said public computer network.

38. System according to claim 34, wherein
said customer computer includes means for establishing a communication channel between the customer computer and the payment system that is separate from said public computer network.

39. System according to claim 34, wherein
the payment system is connected to the payment authorization channel through a communication channel that is separate from the communication said public computer network, such as a dedicated line.

40. System according to claim 34, wherein
the customer computer further includes means for encrypting any information transferred from said customer computer to the payment center.

41. System according to claim 34, wherein
the vendor computer further includes means for receiving said voucher from said customer computer in exchange for the delivery of the ordered goods and/or services and means for forwarding this voucher to the payment system as part of the claim that the delivery of the ordered goods and/or services has been made.

42. System according to claim 34, wherein
the payment system further includes means for generating information that can be used to verify the authenticity of the information representing the voucher, such as a checksum, a part of the voucher information or a key for decrypting information hidden in the voucher, as well as means for sending this information as part of the delivery approval information.

43. System according to claim 34, wherein
the payment system further includes means for generating a digital signature that enables the vendor to confirm that the approval information originated with the payment system.

44. System according to claim 34, wherein
the payment system further includes means for debiting the customer and crediting the vendor in accordance with the payment information and any additional information including commissions and fees.

45. System according to claim 44, wherein

said payment information includes additional information regarding fees to any third party and said payment system further includes means for crediting said third parties in accordance with said additional information.

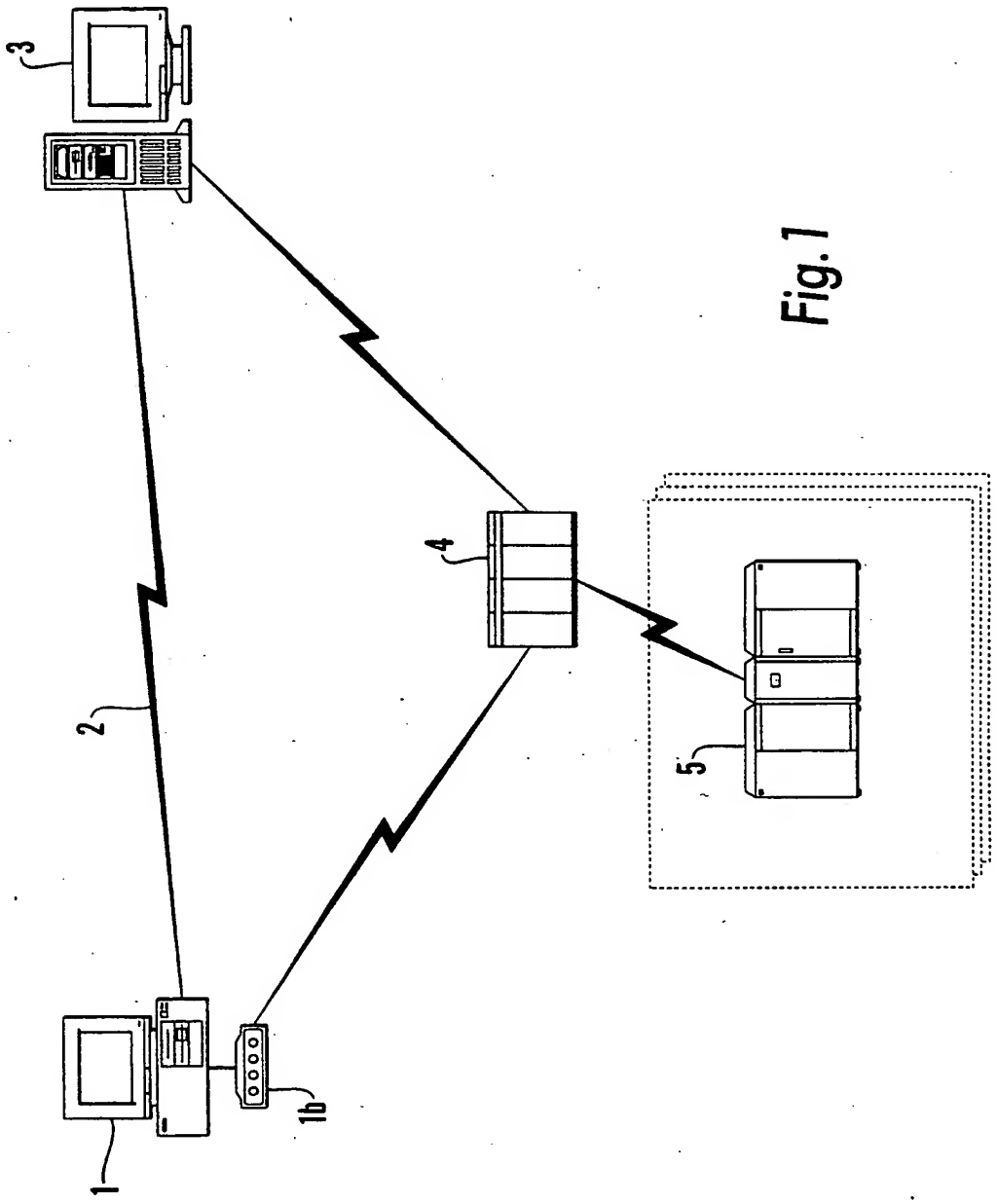


Fig.1

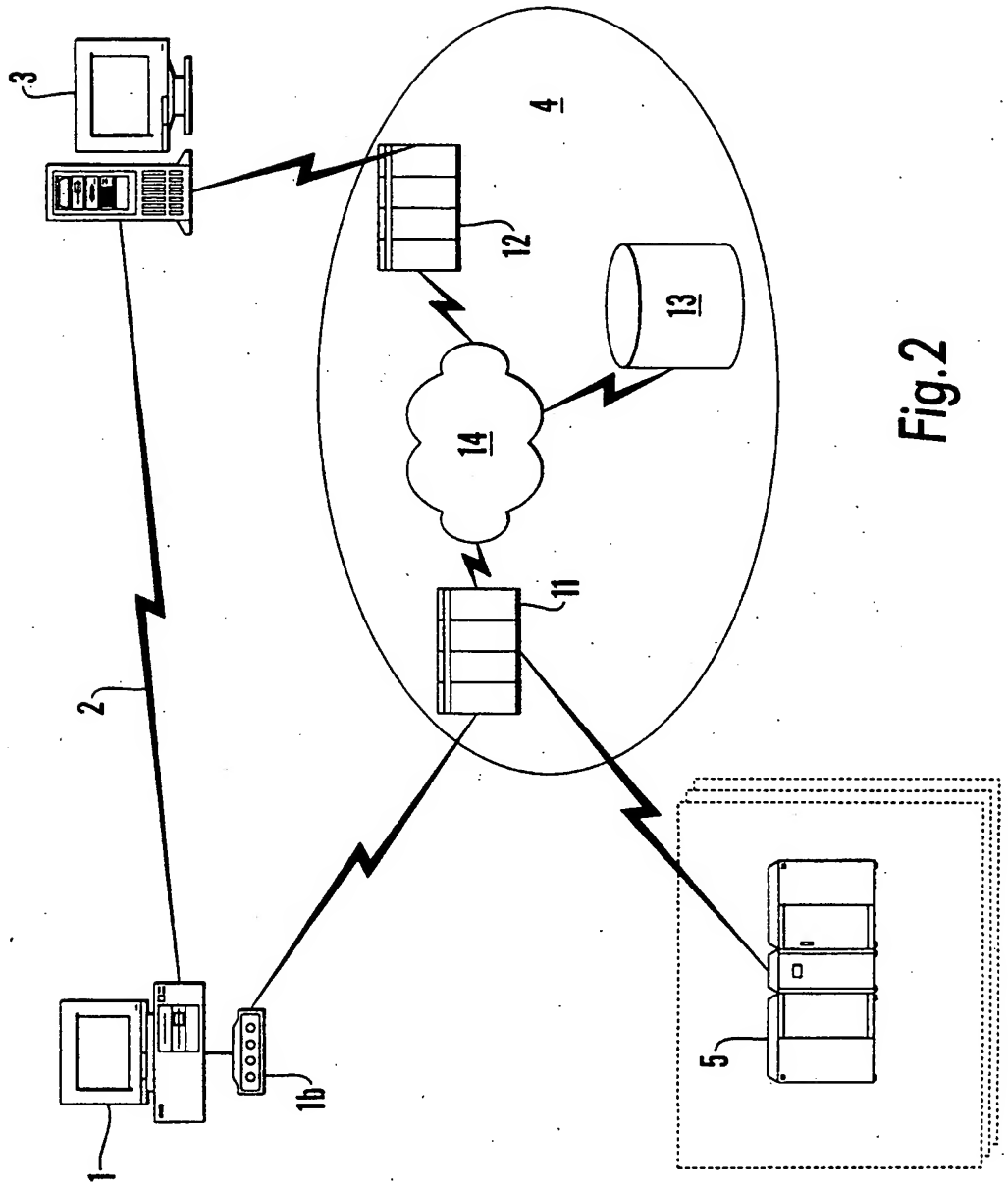


Fig.2

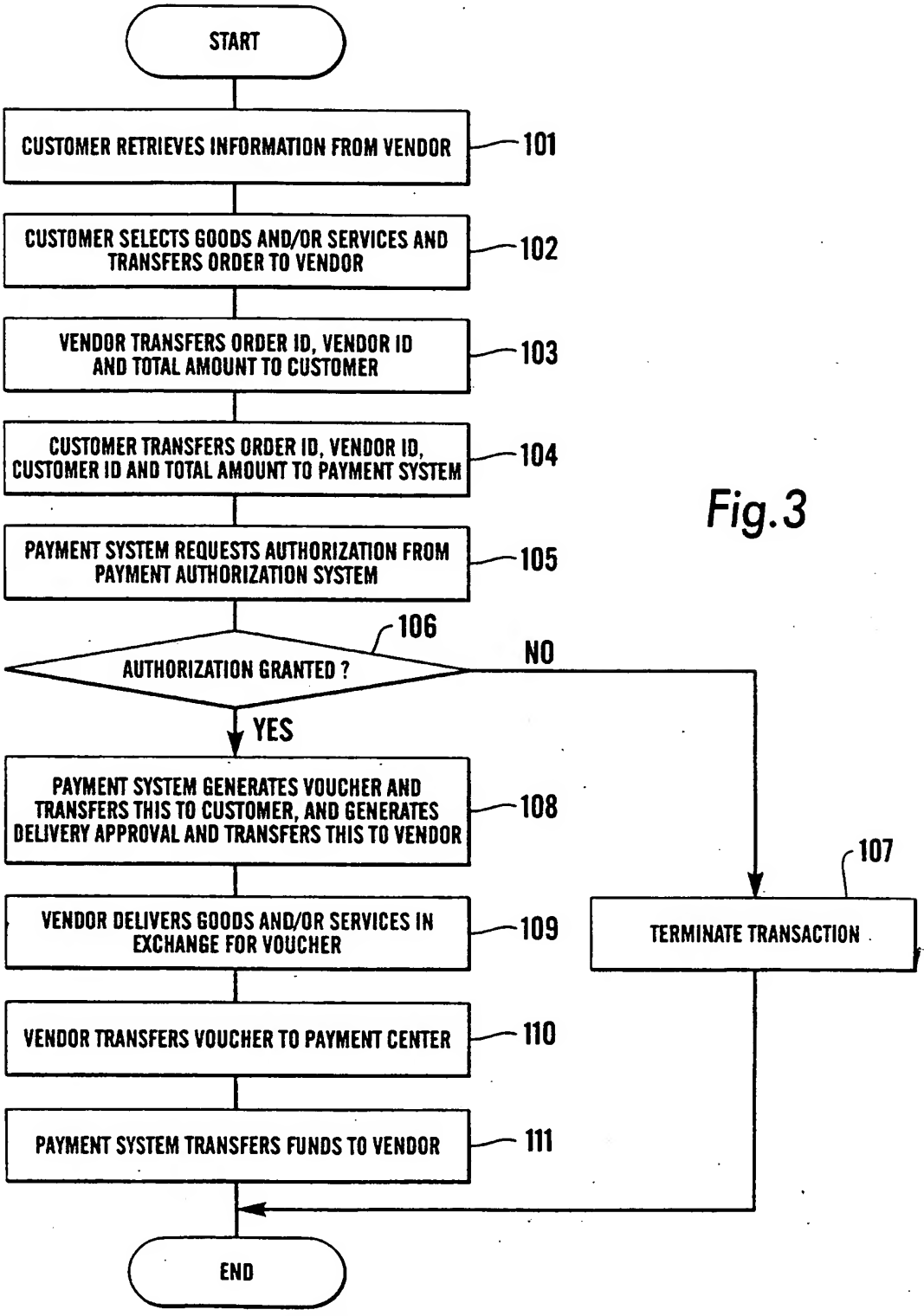

START
CUSTOMER RETRIEVES INFORMATION FROM VENDOR
101
CUSTOMER SELECTS GOODS AND/OR SERVICES AND TRANSFERS ORDER TO VENDOR
102
VENDOR TRANSFERS ORDER ID, VENDOR ID AND TOTAL AMOUNT TO CUSTOMER
103
CUSTOMER TRANSFERS ORDER ID, VENDOR ID, CUSTOMER ID AND TOTAL AMOUNT TO PAYMENT SYSTEM
104
PAYMENT SYSTEM REQUESTS AUTHORIZATION FROM PAYMENT AUTHORIZATION SYSTEM
105
106
AUTHORIZATION GRANTED ?
NO
YES
PAYMENT SYSTEM GENERATES VOUCHER AND TRANSFERS THIS TO CUSTOMER, AND GENERATES DELIVERY APPROVAL AND TRANSFERS THIS TO VENDOR
108
107
VENDOR DELIVERS GOODS AND/OR SERVICES IN EXCHANGE FOR VOUCHER
109
TERMINATE TRANSACTION
VENDOR TRANSFERS VOUCHER TO PAYMENT CENTER
110
PAYMENT SYSTEM TRANSFERS FUNDS TO VENDOR
111
END

Fig.3

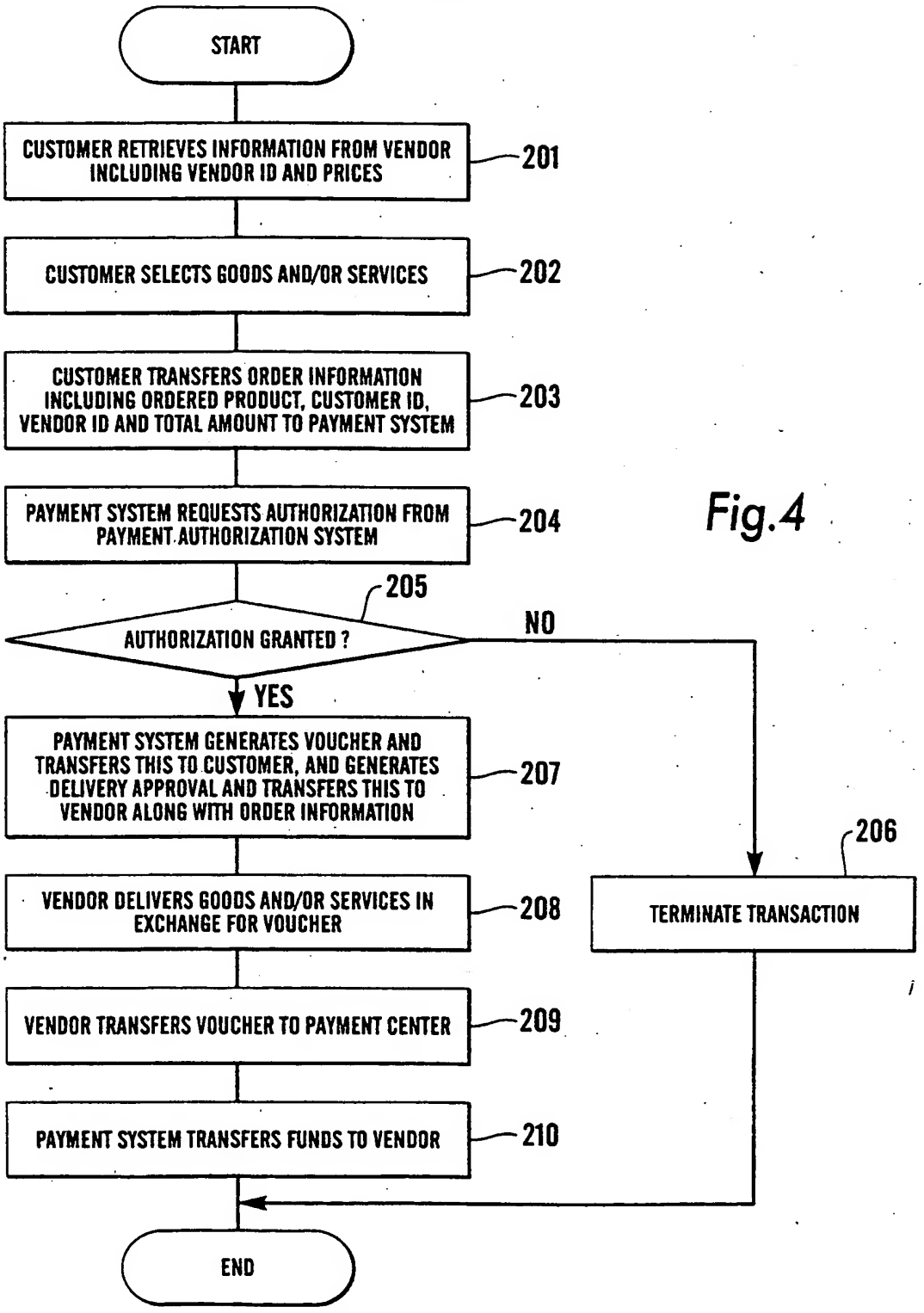

START
CUSTOMER RETRIEVES INFORMATION FROM VENDOR INCLUDING VENDOR ID AND PRICES
201
CUSTOMER SELECTS GOODS AND/OR SERVICES
202
CUSTOMER TRANSFERS ORDER INFORMATION INCLUDING ORDERED PRODUCT, CUSTOMER ID, VENDOR ID AND TOTAL AMOUNT TO PAYMENT SYSTEM
203
PAYMENT SYSTEM REQUESTS AUTHORIZATION FROM PAYMENT AUTHORIZATION SYSTEM
204
205
AUTHORIZATION GRANTED ?
NO
YES
PAYMENT SYSTEM GENERATES VOUCHER AND TRANSFERS THIS TO CUSTOMER, AND GENERATES DELIVERY APPROVAL AND TRANSFERS THIS TO VENDOR ALONG WITH ORDER INFORMATION
207
206
VENDOR DELIVERS GOODS AND/OR SERVICES IN EXCHANGE FOR VOUCHER
208
TERMINATE TRANSACTION
VENDOR TRANSFERS VOUCHER TO PAYMENT CENTER
209
PAYMENT SYSTEM TRANSFERS FUNDS TO VENDOR
210
END

Fig.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 00/00092

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G06F 17/60
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9908218 A (TRIVNET LTD.), 18 February 1999 (18.02.99), page 3, line 2 - page 7, line 29; page 27, line 25 - page 28, line 19; page 30, line 11 - line 19, figures 1-11, claims 1,10	1-46
X	US 5822737 A (OGRAM), 13 October 1998 (13.10.98), column 1, line 43 - column 3, line 19, figure 4, claims 1,22, abstract	1-46
X	WO 9822915 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY), 28 May 1998 (28.05.98), page 2, line 16 - line 30, figures 1,8, claim 1, abstract	1-46

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 June 2000	18. 07. 2000

Name and mailing address of the International Searching Authority
European Patent Office P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel(+31-70)340-2040, Tx 31 651 epo nl,
Fax(+31-70)340-3016

Authorized officer
JAN SILFVERLING/EE
Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 00/00092

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	US 5903880 A (BIFFAR), 11 May 1999 (11.05.99), column 3, line 14 - column 4, line 33, claim 1, abstract -- --------	1-46

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO00/00092

Box I **Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 1-46
because they relate to subject matter not required to be searched by this Authority, namely:

Schemes, rules or methods of doing business. After all search has been performed and a searchreport had been established.

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).:

Box II **Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims: it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

International application No.
PCT/NO 00/00092

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9908218 A	18/02/99	AU 8644298 A	01/03/99
		US 5899980 A	04/05/99
US 5822737 A	13/10/98	US 5963917 A	05/10/99
WO 9822915 A1	28/05/98	AU 4957197 A	10/06/98
		EP 0941524 A	15/09/99
		GB 9624127 D	00/00/00
US 5903880 A	11/05/99	NONE	